VECTRA

FORESCOUT

Gain real-time visibility and automated response with Vectra and Forescout

CHALLENGE

Organizations need greater visibility into threats as well as the devices and accounts in their network to respond effectively against cyberattacks.

SOLUTION

The integration of the Cognito network detection and response platform from Vectra with the Forescout device visibility and control platform provides inside-the-network threat detection and response, a critical layer of defense in today's security infrastructure.

BENEFITS

- Automate network defense. Combine behavior-based threat detection with real-time enforcement.
- Empower security analysts. Respond to threats using simple event tags.
- Trigger different network actions. Take action based on type of threat, risk and certainty.
- Enforce device compliance. Automate remediation and response for noncompliant devices.

Inside-the-network threat detection

As the scale and sophistication of network threats continue to increase, businesses need greater visibility into threats as well as the devices and accounts in their network. To respond effectively against these cyberattacks, a modern security approach must be built on automated, actionable intelligence that can be easily shared between systems.

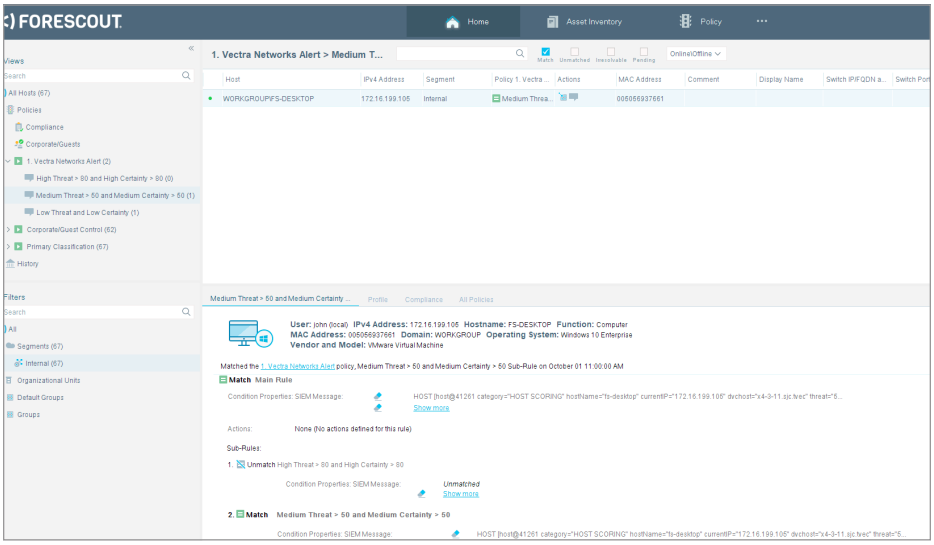
Forescout and Vectra work together to provide inside-the-network threat detection and response as a critical layer of defense in today's security infrastructure.

The Forescout platform delivers absolute real-time visibility and control of all the diverse types of devices connected to the enterprise network.

The Cognito™ network detection and response platform from Vectra constantly analyzes network traffic to reveal all phases of an active cyberattack.

The Cognito platform surfaces threat behaviors including hidden command and control (C&C) communications, internal reconnaissance, lateral movement, botnet fraud, ransomware and data exfiltration.

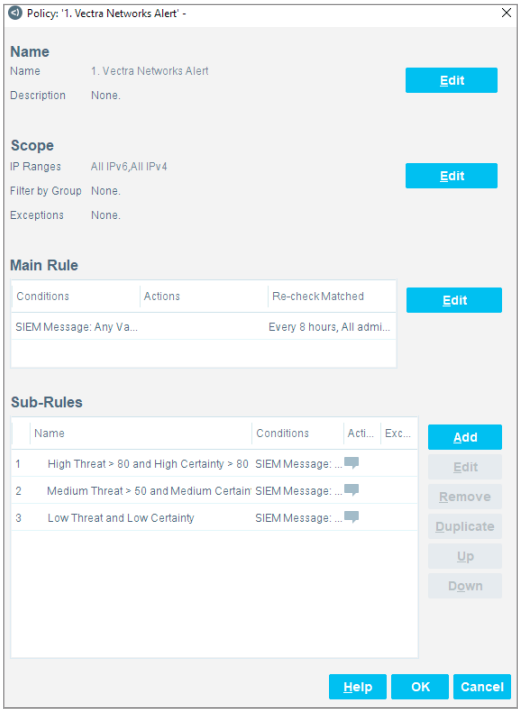
Cognito scores and ranks network hosts by risk. To enable faster investigation and response, all malicious behaviors are automatically associated to the physical network host, even if the IP address changes.



Automate defenses based on risk

When Cognito identifies an infected device, its IP address and threat certainty are pushed to Forescout.

The integration then enables automated remediation actions including dynamic segmentation, quarantining infected devices, blocking communication with a C&C server, and preventing data exfiltration across all device types and network tiers.



Forescout can be configured to take action based on risk scores. For example, a low-risk score could merit segmenting a host to an inspection VLAN with restricted access for further monitoring and investigation.

A higher risk score could trigger an automated quarantine, cutting off all communication to avoid attacker lateral movement and data exfiltration.

Forescout device visibility and control platform enables automated response to quarantine infected devices and block communication with a C&C server. This integration provides a foundation that secures against the broadest spectrum of threats.

Automated remediation actions could follow or trigger orchestration events like patch management through other system integrations with Forescout. Once all vulnerabilities are addressed, the device could be automatically allowed back onto the network per policy.

A new class of defense

With this joint solution, Vectra and Forescout have created a new class of defense. By combining data science and machine learning, Vectra provides the fastest, most efficient way to find and stop attackers once they are inside a network.

About Vectra

Vectra is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time.

Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.

About Forescout

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. As of June 30, 2019, 3,400 customers in over 85 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai